Міністерство освіти і науки України

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

«Криптографія»

Лабораторна робота №3.

«Криптоаналіз афінної біграмної підстановки»

Виконали:

Варіант - **5**

студенти гр. ФБ-92

Кудряшов М.О. та Курганський Л. С.

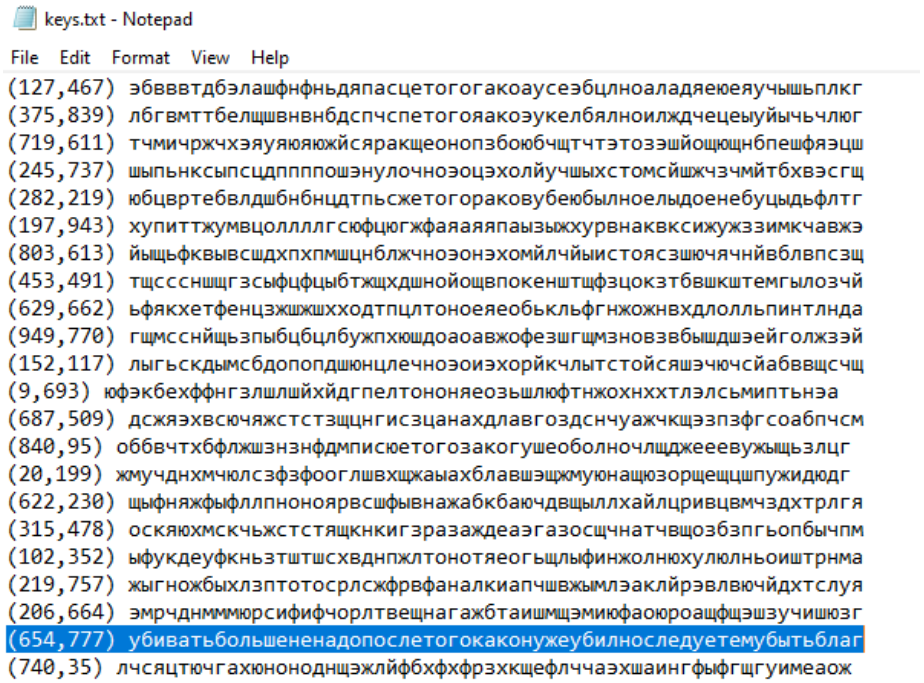
Мета роботи: Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Загальний код програми знаходиться в файлі "main.py"

Хід роботи

1. При запуску програма запитує варіант;
2. Відбувається зчитування зашифрованого тексту, його очищення;
3. Створення на основі тексту біграм;
4. Пошук найпопулярніших біграм;
5. Визначення можливих перестановок популярних біграм з тексту із популярними біграмами з мови;
6. Визначення комбінацій пар біграм для складення системи порівнянь;
7. Розв’язки можливих систем і визначення ключів (a, b);
8. Підбір ключів на основі не великої частини тексту;
9. Аналіз розшифрованих текстів і ключів;
10. Пошук змістового тексту і ключа, розшифрування всього тексту.

Аналіз відбувається після фільтрації програмою вручну, переглядом варіантів:



Розшифрований текст (654, 777):

убивать больше не надо после того как он уже убил но следует ему быть благодарным иначе пришлось бы убивать самому это не одно лишь доброе сострадание это ото ж дествление на основании одинаковых импульсов к убийству собственного воря лишь в минимальной степени смещенный нарциссизм эти ческая ценность этой доброты эти мне оспаривается может быть это вообще механизм нашего доброго участия по отношению к другому человеку особенно ясно проступающий в чрезвычайном случае обремененного сознания своей вины писателя нет сомнения что эта симпатия по причине отож дествления решительно определила выбор материала достоевского но сначала они з эгоистических побуждений выводило бы к новенного преступника политического и религиозного прежде чем к концу своей жизни вернуться к первопреступнику котце убийцеи сделать в его лице свое поэтическое признание опубликование его посмертного наследия и дневников его жены ярко осветило один эпизод его жизни то время когда достоевский в германии было буре ваемигорной страстью достоевский за рулеткой явный припадок патологической страсти который не поддается иной оценке ни с какой стороны не было недостатка в оправданиях этого странного и недостойного поведения чувство виныкак это нередко бывает у невротиков нашло конкретнуюзаменувобремененностидолгамиидостоевскиймоготговариватьсятемчтоонпривыигрыше получилбывозможностьвернутьсяврассиюизбежавзаключениявтюрьмукредитораминоэтобылтолькоп редлогдостоевскийбылдостаточнопроницателенчтобыэтопонятьидостаточночестенчтобывэтомпризн атьсяонзналчтоглавнымбылаиграсамапосебевсеподробностиегообусловленногопервичнымипозывам ибезрассудногоповеденияслужаттомудоказательствомиещекоечемуиномуоннеуспокаивалсяпоканет ерялвсегоиграбыладлянеготакжесредствомсамонаказаниянесчетноеколичествораздавалонмолодой женесловоиличестноесловобольшенеиграть илинеиграть вэтотденьионнарушалэтословокаконарасска зываетпочтивсегдаеслионсвоимипроигрышамидоводилсебяиеедокрайнебедственногоположенияэто служилодлянегоещеоднимпатологическимудовлетворениемонмогпереднеюпоноситьиунижатьсебяп роситьеепрезиратьегораскаиватьсявтомчтоонавышлазамужзанегостарогогрешникаипослевсейэтойра згрузкисовестинаследующийденьиграначиналасьсноваимолодаяженапривыклакэтомуциклутаккаказа метилачтотоотчеговдействительноститолькоиможнобылоожидатьспасенияписательствоникогданепр одвигалосьвпередлучшечемпослепотеривсегоизакладыванияпоследнегоимуществасвязивсегоэтогоо наконечнонепонималакогдаегочувствовиныбылоудовлетворенонаказаниямиккоторымонсамсебяпри говорилтогдаисчезалазатрудненностьвработетогдаонпозволялсебесделатьнесколькошаговнапутикус пехурассматриваярассказболеемолодогописателянетрудноугадаткакиедавнопозабытыедетскиепере живаниянаходятвыявлениявигорнойстрастиустефанацвейгапосвятившегомеждупрочимдостоевскому одинизсвоихочерковтримастеравсборникесмятениечувствестьновелладвадцатьчетыречасавжизниже нщиныэтотмаленькийшедеврпоказываеткакбудтолишьтокакимбезответственнымсуществомявляется женщинаинакакиеудивительныедлянеесамойзаконо нарушенияеетолкаетнеожиданноежизненноевп ечатлениеноновеллаэтаеслиподвергнутьеепсихоаналитическомутолкованиюговоритоднакобезтакойо правдывающейтенденциигораздобольшепоказываетсовсеминоеобщечеловеческоеилискореообщем ужскоеитакоетолкованиестольявноподсказаночтонетвозможностиегонедопуститьдлясущностихудож ественноготворчествахарактерночтописательскоторымменясвязываютдружескиеотношениявответна моирасспросыутверждалчтоупомянутоетолкованиеемучуждоивовсеневходиловегонамерениянесмот рянаточтоврассказвплетенынекоторыедеталикакбырассчитанныенаточтобыуказыватьнатайныйследв этойновеллевеликосветскаяпожилаядамаповеряетписателюотомчтоейпришлосьпережитьболеедвад цатилеттомуназадраноовдовевшаяматьдвухсыновейкоторыевнейболеененуждалисьотказавшаясяотк

акихбытонибылонадежднасороквторомгодужизнионапопадаетвовремяодногоизсвоихбесцельныхпутешествийвигорныйзалмонакскогоказиногдесредивсехдиковинеевниманиеприковываютдверукикоторыеспотрясающейнепосредственностьюисилойотражаютвсепереживаемыенесчастнымигрокомчувстварукиэтирукикрасивогоюношиписателькакбыбезовсякогоумысладелаетегоровесникомстаршегосынанаблюдающейзаигройженщиныпотерявшеговсеивглубочайшемотчаяниипокидающегозалчтобывпарке покончитьсосвоеюбезнадежнойжизньюнеизяснимаясимпатиязаставляетженщинуследоватьзаюношейвпредпринятьвседляегоспасенияонпринимаетеезаоднуизмногочисленныхвтомгороденавязчивыхженщинихочетотнееотделатьсяноонанепокидаетегоивынужденавконцеконцоввсилусложившихсяобстоятельствостатьсявегономереотеляиразделитьегопостельпослеэтойимпровизированнойлюбовнойночионавелитказалосьбыуспокоившемусяюношедатьейторжественноеобещаниечтоонникогдабольшенебудетигратьснабжаетегоденьгаминаобратныйпутьисосвоейстороныдаетобещаниевстретитьсяснимпередуходомпоезданавокзаленозатемвнейпробуждаетсябольшаянежностькюношеонаготовапожертвоватьвсемчтобытолькосохранитьегодлясебяионарешаетотправитьсяснимвместевпутешествиевместотогочтобыснимпроститьсявсяческиепомехизадерживаютееионаопаздываетнапоездвтоскепоисчезнувшемуюношеонасноваприходитвигорныйдомисвозмущениемобнаруживаеттамтежерукинакануневозбудившиевнейтакуюгорячуюсимпатиюнарушительдолгавернулсякигреонанапоминаетемуобегообещанииноодержимыйстрастьюонбранитсорвавшуюегоигрувелитейубиратьсявонишвыряетденьгикоторымионахотелаеговыкупитьопозореннаяонапокидаетгородавпоследствииузнаетчтоейнеудалосьспастиегоотсамоубийстваэтаблестящеибезпробеловвмотивировкенаписаннаяновеллаимеетконечноправонасуществованиекактаковаяинеможетнепроизвестиначителябольшоговпечатленияоднакопсихоанализучитчтоонавозникланаосновеумопострояемоговожделенияпериодаполовогосозреванияокаковомвождененииинекоторыевспоминаютсовершенносознательносогласноумопострояемомувождениюматьдолжнасамаввестиюношувполовуюжизньдляспасенияегоотзаслуживающегоопасениявредаонанизмастольчастыесублимирующиехудожественныепроизведениявытекаютизтогожепервоисточникапороконанизмазамещаетсяпорокомигорной страсти ударение поставленное настрастную деятельность рук предательски свидетельствует об этом от воде энергии действительно игорная одержимость является эквивалентом старой потребности вонан измени одним словом кроме слова игра нельзя назвать етееаа

P.s. текст у 5 варіанту трохи дивний, але програма була перевірена на інших варіантах (1, 4) і працює коректно.